Security in Relais

Find information about security for passwords in Relais and options for sending patron credentials.

Security for passwords and the Relais database connection

The connection between the database server and any workstations on which the Relais Windows client is running, e.g., for Login, Print Request, Receive FTP, Delivery Local, is encrypted for customers using the Relais Hosted Service.

The database password is updated to be customer specific.

All passwords in Relais are encrypted so that at no time are any of the passwords used, stored or displayed in the Relais database or any ini or cfg files human readable. This includes all of the following:

- Relais database password
- System related passwords, e.g., those used by automated applications
- All staff, patron (if applicable) and library passwords
- Z39.50 server passwords, e.g., for Libraries Australia and OCLC
- Rapid ILL password
- FTP server password used by the File Transfer Service
- Archive database password used by Purge and Archive
- Any passwords included in the Load Request and Update Patron Records files

AES-128 symmetric encryption is used.

Security options for sending patron credentials

There are two options available for ensuring the patron information you pass to Relais in a URL, either to Discovery or to a Portal Request form, is not visible.

Option 1: Use public-key for asymmetric key encryption

Encrypt the patron credentials using a public-key (PEM format) for asymmetric key encryption prior to constructing the URL to pass to Relais.

The following OpenURL tags can be encrypted:

- PI : Patron ID
- PS : Patron surname
- UL : User login
• **UP**: User password
• **RK**: Record key

On receipt of the URL with the patron credentials Relais calls the Authentication service. The Authentication service:

• Uses the Library Symbol, patron credentials and the API key configured for your library.
• Validates your API key, un-encrypts the patron credentials.
• If NCIP is in use:
  ◦ Uses the library symbol and the credentials to do an NCIP Lookup User to retrieve the patron information.
• If NCIP is not in use:
  ◦ Uses the library symbol and patron credentials id to look up the patron record in the Relais database
• Creates an **aid** or authorization id.
  ◦ The **aid** is used when making calls in Relais, such as to the Requestability and Add Request services.

### Examples

1. If you provide the patron’s barcode for use in an NCIP Lookup User message
   ◦ https://demo.relais-host.com/user/login.html?group=patron&LS=OORII&PI=encrypted_patron_id&etc...

2. If you provide the patron’s barcode and surname for use in an NCIP Lookup User message
   ◦ https://demo.relais-host.com/user/login.html?group=patron&LS=OORII&PL=encrypted_patron_id&PS=encrypted_patron_sumame&etc...

3. If you provide the patron’s Relais Login and Password
   ◦ https://demo.relais-host.com/user/login.html?group=patron&LS=OORII&UL=encrypted_user_login&UP=encrypted_user_password&etc...

Caution: To safeguard against replay attack the plain text of any of the attributes you will encrypt (patron id, patron surname, etc.) must have the UTC datetime appended to it in the following format before the entire string is encrypted:

```
actual_value|yyyyMMdd HHmmss
```

For example: "12391334|20150706 163237", where

12391334 = patron id in plain text
20150706 163237 = current UTC datetime. * Note there is a space between the yyyyMMdd and the HHmmss

When doing the encryption be sure to encrypt the **full** text string, e.g., "12391334|20150706 163237"

After the value is un-encrypted, the plain text is split using the `'|'` character. If `'|'` is not found the Authentication service will fail.

The UTC datetime in the encrypted text must be within the last 5 minutes of the current UTC time. For example, if the UTC datetime in the encrypted text + 5 minutes is before the current UTC datetime, the Authentication process will fail. Similarly, if the UTC datetime in the encrypted text is after the current UTC datetime the Authentication process will fail.

Note: See [Encryption](https://help.oclc.org/Resource_Sharing/Relais_ILL/Authentication/Security_in_Relais) for instructions and sample code for encrypting text using the public-key.
Note: To use a public-key for asymmetric key encryption please contact OCLC Support and request a public-key. You will be given two public-keys: one for testing purposes and your actual public-key for use in production.

**Testing public-key encryption in an URL**

To test your encryption use one of the following three links. Please use the appropriate link depending on what patron credentials you are passing to Relais.

<table>
<thead>
<tr>
<th>OPENURL TAG SENT</th>
<th>TEST URL</th>
<th>INSTRUCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>PI (patron ID)</td>
<td><a href="https://sandbox.relais-host.com/user/login.html?group=patron&amp;LS=LIBA&amp;PI=">https://sandbox.relais-host.com/user/login.html?group=patron&amp;LS=LIBA&amp;PI=</a></td>
<td>• Replace encrypted-dummy-patron-ID with the encrypted value for patron ID = 123456A</td>
</tr>
<tr>
<td></td>
<td>encrypted-patron-ID</td>
<td></td>
</tr>
<tr>
<td>PI (patron ID) and PS (patron surname)</td>
<td><a href="https://sandbox.relais-host.com/user/login.html?group=patron&amp;LS=LIBB&amp;PI=encrypted-patron-ID&amp;PS=encrypted-patron-surname">https://sandbox.relais-host.com/user/login.html?group=patron&amp;LS=LIBB&amp;PI=encrypted-patron-ID&amp;PS=encrypted-patron-surname</a></td>
<td>• Replace encrypted-patron-ID with the encrypted value for patron ID = 123456B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Replace encrypted-patron-surname with the encrypted value for patron surname = SURNAMEB</td>
</tr>
<tr>
<td>UL (user login) and UP (user password)</td>
<td><a href="https://sandbox.relais-host.com/user/login.html?group=patron&amp;LS=LIBC&amp;UL=encrypted-user-login&amp;UP=encrypted-user-password">https://sandbox.relais-host.com/user/login.html?group=patron&amp;LS=LIBC&amp;UL=encrypted-user-login&amp;UP=encrypted-user-password</a></td>
<td>• Replace encrypted-user-login with the encrypted value for user login = loginC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Replace encrypted-user-password with the encrypted value for user password = passwordC</td>
</tr>
</tbody>
</table>

If, using the appropriate link, you are able to login and the My Requests > Open Requests page displays then your encryption is working.

**Caution:** Once you have completed testing and encryption is working, then contact OCLC Support to advise which combination of patron credentials you are using so that the switch to use encryption can be made (a configuration change is required in the Relais Portal) and to coordinate the switch to use encryption in production.

**Turn on encryption in production**

Encryption is turned on in production In coordination with staff at Relais international. You will need to:

1. Start using your own specific public-key.
Be sure to use your specific public-key and not the public-key used in testing.

2. Switch your login URL to reflect your own instance of the Relais Portal or Discovery. For example:
   - A login URL for Discovery: https://ezb.relaisd2d.com/?LS=LIBRARYSYMBOL&PI=\${ENCRYPTED-PI-GOES-HERE}
   - A patron link to the Relais Portal: https://acmr.relais-host.com/user/login.html?group=patron&LS=LIBRARYSYMBOL&PI=\${ENCRYPTED-PI-GOES-HERE}

Caution: If you are also using the Relais Discovery web services after the switch to public-key encryption, the calls made to the Relais Authentication service will expect the configured parameters to be encrypted as well.

Option 2: Call the Relais Authentication service to generate an aid

When your application calls the Authentication service a library specific API key and patron credentials must be included. See Authentication for more information.

The following patron information may be encrypted. See Encryption for more information.

- ApiKey
- PatronId
- Surname
- RecordKey
- UserLogin
- UserPassword

The Authentication service returns an ‘aid’. In the URL you pass to Relais, include the ‘aid’ and your library symbol. On receipt of the URL (with the ‘aid’ and the library symbol) Relais calls the Authentication service. The Authentication service:

- uses the library symbol, 'aid' and the API key configured for your library
- validates the ‘aid’ and retrieves the corresponding patron information from the Relais database.
- no NCIP lookup is done
- The ‘aid’ is used when making calls in Relais, e.g., to the Requestability and Add Request services

To use the Authentication service to generate an ‘aid’ please contact OCLC Support and request your API key as well as information regarding how you may test.

For example:

Once you have received the aid from the Authentication Service then it is if you provide the patron's barcode for use in an NCIP Lookup User message

https://HOSTNAME.relais-host.com/user/login.html?group=patron&aid=ajfljalsdjajslfjalalldjldj